



SPACE CYBERSECURITY WEEKLY WATCH

Week 40

September 26 – October 2, 2023

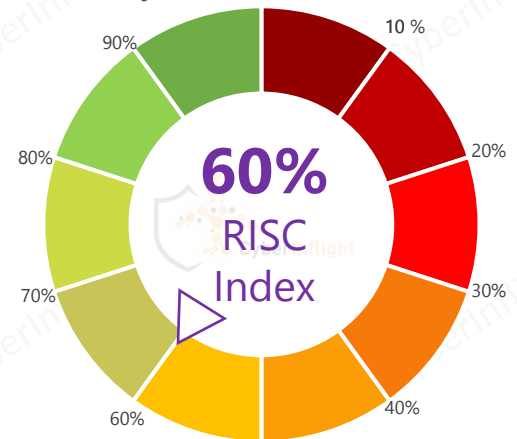
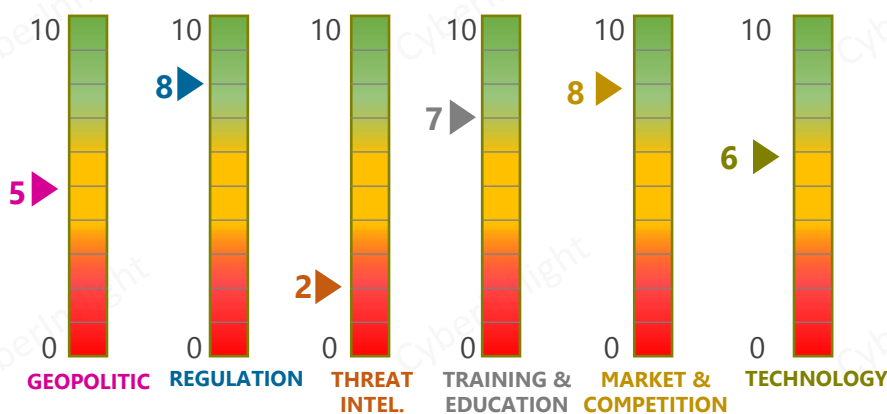
Timeframe : Weekly
of articles identified : 42
Est. time to read : 1 h 35 min

Articles, company's communications, whitepapers, academic works, podcast, and sources not to be missed on the topic of space cybersecurity over a specified timeframe.

- **GEOPOLITIC**
- **REGULATION**
- **THREAT INTELLIGENCE**
- **TRAINING & EDUCATION**
- **MARKET & COMPETITION**
- **TECHNOLOGY**
- ★ **IMPORTANT NEWS**

CYBERINFLIGHT'S NEWS :

★ Introduction of CyberInflight's RISC ★
Resilience Index for Space Cybersecurity



To celebrate the cyber-month, CyberInflight has decided to launch a new feature for its weekly watch: **the Resilience Index for Space Cybersecurity (RISC)**! This cyber resilience index allows us to assess the state of each category identified by CyberInflight. A score is given out of 10 for each section, which is assessed on the information presented in each section. This week, there was more important regulatory news than usual, allowing us to score well. The same reasoning was applied to Market and Training. There was also more jamming and attack news, explaining the threat intel section's low score. This week we have a 60% RISC Index, which is a relatively good score, but leaves room for improvement!

Overview

This week saw the release of 2 important announcements concerning space cybersecurity regulations. Firstly, the NIST National Cybersecurity Center of Excellence published the final version, NIST IR 8441, of the Cybersecurity Framework Profile for Hybrid Satellite Networks. Also this week, the European Commission launched a Targeted Stakeholder Consultation for an EU Space Law, which runs until November 2, 2023, and envisages common EU rules addressing the safety, resilience and sustainability of space activities and operations.

Earlier this week, the USSF and its partners decided to meet next month to discuss a strategy for supply chain resilience. In terms of threat intelligence, the Russian ransomware group Killnet has claimed responsibility for an attack on several US groups, including Lockheed Martin. CyberInflight also reported on a number of jamming-related news, and several attacks that took place. ESA is organizing a hacking contest to take control of a small rover. On the Market front, the USSF awarded several contracts this week, including the main one with John Hopkins University, to evaluate the software and cybersecurity of ground systems being developed for a new classified satellite network. Finally, on the technology front, L3Harris presented its Protected Tactical Waveform, providing warfighters with long-range, higher-bandwidth communication in the presence of jamming across all domains.



GEOPOLITIC

Space Critical Infrastructure: Breaking the Binary Debate and a Call for Space Council Action

The question for space is not whether space itself is vital, but what functions in space are "critical" that their incapacitation or destruction would have a debilitating effect on the ability to operate and survive in space. #US #CriticalInfrastructure

Link: [https://www.space.com/space-critical-infrastructure-breaking-the-binary-debate-and-a-call-for-space-council-action](#)



The critical role of space technology in improving systems of governance

In the address to the UN, speakers from various countries noted that space technology was not only for sending satellites to orbit the earth and exchanging interplanetary travels. It was also for improving the systems of governance in the country. #UN #Media

Link: [https://www.space.com/space-technology-improving-systems-of-governance](#)



Space Force, partners to craft global supply chain strategy

U.S. Space Force officials will meet next month with industry leaders and key international partners to discuss a strategy for supply chain resiliency. #USSF #SupplyChain

Link: <https://www.defensenews.com/battlefield-tech/space/2023/09/25/space-force-partners-to-craft-global-supply-chain-strategy/>



UK London arms fair, global war fears are good for business

These warlike satellite communications were also seen responding to a series of other satellite systems of different types in London, giving them a better resistance to jamming or other disruptive actions. #London #Space

Link: [https://www.space.com/space-uk-london-arms-fair-global-war-fears-good-business-2023-09-25](#)



REGULATION



NIST NCCoE Publishes Final NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks

The NIST National Cybersecurity Center of Excellence (NCCoE) has published Final NIST IR 8441, Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). #NIST #Cybersecurity

Link: <https://www.nccoe.nist.gov/news-insights/nist-nccoe-publishes-final-nist-ir-8441-cybersecurity-framework-profile-hybrid>



Portugal Discusses Plan for Defending Space Systems

Last month, the Portuguese finally responded to congressional inquiries regarding Portugal's updated report entitled "Space Policy Review and Strategy on Protection of Satellites" in broad brush details. #EU #Space

Link: [https://www.space.com/portugal-discusses-plan-for-defending-space-systems-2023-09-25](#)



Germany adopts new space strategy

The German government on Wednesday adopted a new space strategy that focuses on promoting private sector initiatives in space. #Germany #SpaceStrategy

Link: [https://www.space.com/germany-adopts-new-space-strategy-2023-09-25](#)



Launch of a Targeted Stakeholder Consultation for an EU Space Law

The Letter of Intent includes an initiative for an EU Space Law (EUSL). The legislative proposal could be adopted by the Commission in the first trimester of 2024. It envisages common EU rules addressing the safety, resilience and sustainability of space activities and operations. It intends to avoid and remove fragmentation and barriers across the single market caused by the heterogeneity or lack of national space legislations, while ensuring the competitiveness of the European space sector in an international trade context. #EU #SpaceLaw

Link: https://defence-industry-space.ec.europa.eu/targeted-consultation-eu-space-law_en





THREAT INTELLIGENCE



Cyber Attack on Lockheed Martin: Killnet Targets US Defense Giant Amid Geopolitical Tensions



Lockheed Martin, an international aerospace, arms, defense, and information security corporation is the latest victim of the Killnet ransomware group. The Russian hacktivist group named not one but two U.S. organizations in a Telegram message. They named the Army Transport Corps alongside the claim of cyber attack on Lockheed Martin. **#Russia #Killnet**

Link: <https://theycyberexpress.com/cyber-attack-on-lockheed-martin-target-us/>

Russian e-war system 'likely' behind Ben Gurion disruptions



The Israel Airports Authority has stated that "unknown factors" are disrupting the GPS systems of planes landing at Ben Gurion Airport in recent months. The cause for the disruption is highly likely to be Russian electronic warfare systems. **#Israel #CyberWarfare**

Link: <https://www.washingtonpost.com/technology/2023/09/26/israel-airports-gps-disruptions-likely-russian-attacks/>

Electronic GPS 'spoofing' behind civilian jet navigation failures over Iraq

False electronic signals including satellite data from Global Positioning System satellites recently caused complete navigation failures for 12 aircraft flights over Iraq, according to a private aircraft security group. **#SpoofingGPS**

Link: <https://www.washingtonpost.com/technology/2023/09/26/aircraft-navigation-failures-likely-russian-attacks/>

Ransomware attack by Eltan



Eltan Ransomware group has announced MITRE ATT&CK engineering on the victim list. **#Ransomware**

Link: <https://www.cyberint.com/2023/09/26/eltan-ransomware-attack/>

DDoS attack on the NASA website



The post states that the NASA website has been targeted by a DDoS attack carried out by a threat actor known as DDoS-01. The post provides proof of the downtime of the website and includes a link to a report showing the details of the attack. The post was published on a Telegram channel by the threat actor. The victims of the attack are identified as the NASA website with the attack affecting the availability of the site. The post categorizes this incident as a DDoS attack and mentions that the targeted industry is Aviation & Aerospace, with the organization being NASA. The attack is said to have taken place in the USA. **#NASA #DDoS**

Link: <https://www.cyberint.com/2023/09/26/nasa-ddos-attack/>

AI systems need to be hardened: Officials, industry sound the alarm on quantum threat to encryption



New "quantum-resistant" encryption standards won't be finalized until next year, but officials and experts say agencies and industry should start hunting vulnerabilities hidden in their software and hardware, including embedded chips with tiny AI systems. **#AI #Quantum**

Link: <https://www.washingtonpost.com/technology/2023/09/26/ai-systems-need-to-be-hardened-officials-industry-sound-the-alarm-on-quantum-threat-to-encryption/>

North Korean gov't hackers targeted aerospace company in Spain



Hackers connected to a notorious group on behalf of the North Korean government reportedly attacked an aerospace company in Spain, according to researchers at security company CIRT. **#CyberWarfare #NorthKorea**

Link: <https://www.cyberint.com/2023/09/26/north-korean-hackers-targeted-aerospace-company-in-spain/>

GPS jamming quite routine on long haul flights, spoofing isn't instantly apparent



The US Federal Aviation Administration (FAA) issued a notice that long-haul flights - GPS jamming and spoofing poses safety risk. Potential spoofing activities reported by various civil air operators in Iraq and Azerbaijan pose flight risk to civil aviation operations in the Baghdad and Baku flight information regions (FIR), the US civil aviation regulator warned. **#SpoofingGPS**

Link: <https://www.faa.gov/press-releases/2023/09/26/2023092601>

Russian GPS 'jamming' causing collision risk in Black Sea, Romania says



Romania has claimed Russia is "deliberately and constantly" jamming GPS communications across its territorial waters, this is causing a risk of collisions in the Black Sea, according to army chief of staff General Daniel Petrescu. **#JammingGPS**

Link: <https://www.balkaninsider.com/en/ro/russia-gps-jamming-causing-collision-risk-in-black-sea-romanian-says/>

Satellite Risks: Navigating & Transforming Risk Environment

Today our reliance on satellites is such that without them many business sectors would be brought to a standstill and the world economy would likely come to a halt. To keep the question - how prepared are satellite operators, institutions and governments to mitigate the risks of malicious actions against satellites? **#Space #Cyberwarfare**

Link: <https://www.balkaninsider.com/en/ro/satellite-risks-navigating-transforming-risk-environment/>



TRAINING & EDUCATION



PWN THE ROVER - Hacking Contest

The contest allows to take control of a small robotic asset and navigate through obstacles within the station. The goal is to repair the malfunctioning systems, solve challenges, and protect your rover from cyber attacks. **#ESA #Contest**

Link: <https://www.pwn-the-rover.space/>



Want to hack a satellite?

The French Space Agency (CNES) is looking for 1000 Hackers for the HackSat Challenge in just over three weeks in order to play and learn as well. **#PwnedSatellite**

Link: <https://www.cnes.fr/fr/actualites/1000-hackers-cherchent-a-hacker-une-satellite-20230926>

Global industry gathered in Norway to test robustness

Over 2000 participants from 40 companies and 15 countries worldwide gathered in Norway to test the robustness of their systems. Through the week, satellite-based equipment in cars, drones, airplanes, ferries and ships were exposed to jamming, spoofing and man-in-the-middle attacks. **#SpaceSecurity**

Link: <https://www.space.com/20230926-robustness-test-norway>



Reflecting on a productive day with the SPO Bundesagentur für Luftfahrt's visit to SESO

Key points from the SPO Operations, Engineering & Space Safety about the visit to SESO. The SPO Bundesagentur für Luftfahrt expressed interest in our cybersecurity strategies. We shared our progress in establishing a dedicated Cyber Security Center for Operations at SESO, strengthening existing security protocols. **#ESA**

Link: https://www.esa.int/esaoc/230926_spo_operations_eng_space_safety_visit_seso



Webinar - Mastering GNSS Timing Resilience: The secrets to secure GNSS timing and synchronization

Webinar by Spectracore on September 26, 2023 on the importance of using GNSS for timing and critical about the latest techniques and technologies which ensure secure and accurate system operation. **#Webinar #SpaceSecurity**

Link: <https://www.spectracore.com/newsroom/webinars/webinar-mastering-gnss-timing-and-synchronization>



Our space "Israel is interested in space weapons. Every one of our satellites is a machine of war" statement by Avner, head of the Space and Satellite Administration within the Directorate for Defense Research and Development (DRD) at the Ministry of Defense, taken from a talk at the launch of the OREX-12 satellite. Discusses the plan for the day with both large and small satellites, and explains why he believes competition is essential. **#SpaceSecurity**

Link: <https://www.ard.gov.il/press/2023/09/26/01>



Workshop on the Security of Space and Satellite Systems

Speakers will bring together academic researchers, industry professionals, and government representatives to contribute to new theories, technologies, and systems for cybersecurity challenges in space and on the ground. Speakers will be from Los Angeles, CA in conjunction with the Network and Distributed System Security Symposium (NDSS) 2024. **#Conference #SS**

Link: <https://www.ndss.csl.cmu.edu/>



The Final Frontier: Fortifying Cyber Resilience for the Commercial Space Industry

White Paper about the developing commercial space industry. **#Whitepaper #SpaceIndustry**

Link: <https://www.space.com/20230926-white-paper-fortifying-cyber-resilience-for-commercial-space-industry>

Space Economy Summit

Economic Impact's Space Economy Summit will serve as a crucial platform to connect the space industry with mainstream sectors. The burgeoning space economy offers huge potential for commercial, social and environmental progress. The summit will take place on October 11th in Los Angeles, followed by an online event on October 12th. **#Webinar #SpaceEconomy**

Link: <https://www.economicimpact.com/space-economy-summit>



Securing the Final Frontier: Cybersecurity in Space Technology

As we witness significant growth in investment within this sector and increasing dependence on it in our daily lives, it becomes abundantly clear that factors such as cybersecurity in space and the associated risks can no longer be ignored. **#Space #Cybersecurity**

Link: <https://theplanet.com/cybersecurity-in-space-technology-implications/>



MARKET & COMPETITION



Space Force selects university partner to evaluate classified ground systems software

The Space Force awarded a \$10 million contract to the Johns Hopkins University Applied Physics Lab to evaluate the software and cybersecurity of ground systems being developed for a new classified satellite network.

#USSF #JohnsHopkins

Link: <https://spacenews.com/space-force-selects-university-partner-to-evaluate-classified-ground-systems-software/>



OneWeb to Collaborate on PNT Capabilities With the UK National Physical Laboratory

The United Kingdom's National Physical Laboratory announced Monday that it has signed an MoU with OneWeb to work together on Position, Timing and Navigation (PNT) capabilities in the company's second generation satellite constellation.

Link: <https://www.satellite.com/news/onenweb-to-collaborate-on-pnt-capabilities-with-the-uk-national-physical-laboratory>



BAE Systems to provide secure satellite navigation and positioning for Army infantry and combat vehicles

The BAE Systems W9140 contract delivers precision, accurate positioning, security, and anti-jamming capabilities for space constrained applications.

Link: <https://www.baesystems.com/en-us/press-releases/2023/09/26/bae-systems-satellite-navigation-positioning>



Space Force wrapping up plan to buy C2 software for maneuvering satellites

The Space Force's acquisition office (SFAO) is now "finalizing" a plan to acquire software for command and control (C2) of highly mobile satellites and spacecraft being envisioned for future "direct" space operations, according to Space Daily's sources.

Link: <https://www.space.com/space-force-wrapping-up-plan-to-buy-c2-software-for-maneuvering-satellites>



Edge Security Inc awarded million\$ cybersecurity contract by USSF / SSC

Edge Security Inc has received a \$17 million contract awarded by U.S. Space Force's Space Systems Command (SSC) to offer the company's zero trust access control and data protection across SSC's current and emerging ground and space architectures.

Link: <https://www.satellite.com/news/edge-security-inc-awarded-million-cybersecurity-contract-by-us-space-force>



SpaceX Secures First U.S. Space Force Contract for Starshield Satellite Services

SpaceX has now secured its \$200 million contract with the U.S. Space Force for Starshield services. This contract, valued at up to \$70 million, encompasses end-to-end service delivery via the Starshield constellation, user terminals, ancillary equipment, network management, and related services.

Link: <https://www.spacex.com/press/2023/09/26/spacex-secures-first-us-space-force-contract>



Orbital completes multi-year OneWeb merger after shareholder vote

Orbital has completed its post-merger satellite business with OneWeb's low Earth orbit (LEO) constellation after shareholders voted Sept. 28 in favor of the deal.

Link: <https://www.satellite.com/news/orbital-completes-multi-year-oneweb-merger-after-shareholder-vote>



QNTL + Quantil Labs partner to propel Australian quantum clock technology into space

Quantil Labs recently joined forces with Surrey Satellite Technology Limited (SSTL) through Airbus Australia to further their space knowledge and efforts, a collaboration set to propel Australian quantum technology into space.

Link: <https://www.satellite.com/news/quantil-labs-partner-to-propel-australian-quantum-clock-technology-into-space>



QNTL announces million\$ deal with AFRL

QNTL has expanded the company's relationship with the Air Force Research Lab (AFRL) to deploy two quantum-based sensors for quantum computing and for quantum networking.

Link: <https://www.satellite.com/news/quantil-labs-announces-million-deal-with-afml>



Whitby, WISAT, FOSSA Systems, and BA Lab Join Forces to Revolutionize the Logistics Industry with Innovative Satellite Track & Trace Solution

Whitby, WISAT, FOSSA Systems, and BA Lab have come together to provide a comprehensive, disruptive, trusted, and secure satellite track & trace value proposition for smart containers.

Link: <https://www.globenewswire.com/press-release/2023/09/26/2749074/0/en/Whitby-WISAT-FOSSA-Systems-and-BA-Lab-join-forces-to-revolutionize-the-logistics-industry-with-innovative-satellite-track-trace-solution>





Opportunity: Cybersecurity as Enabler for Secure Satellite Communications and Resilient Applications



This new Space Systems for Safety and Security (4S) Call for Proposals aims to foster the development of innovative satellite communications technologies, products, systems and downstream applications which address these challenges. #ESA #CallforProposal

Link: <https://connectivity.esa.int/opportunity-cybersecurity-enabler-secure-satellite-communications-and-resilient-applications>

TECHNOLOGY

Northrop Grumman Space Force's Satellite Control Network Upgrade With Phase Array Antenna Test Bed

Northrop Grumman demonstrated its phased array antenna system in late August 2022 to set in motion an initial delivery of the first unit by the spring of 2023 to help the U.S. Space Force upgrade its Satellite Control Network (SCN), which is used for ground-based operations. The system is a deployable ground terminal that builds on Northrop's Multi-Beam Antenna System, a phased array technology that streamlines mission operations through agile beamforming. #NorthropGrumman

Link: <https://www.northropgrumman.com/press-releases/2022/northrop-grumman-space-force-satellite-control-network-upgrade-with-phase-array-antenna-test-bed>

ISRO India & ISIRI NPI sign agreement for development of Next-Gen ISIRI In-orbit Primary Reference Star

ISRO India & ISIRI NPI sign agreement for development of Next-Gen ISIRI In-orbit Primary Reference Star (ISIRI-IRS) for deep space navigation of telecom networks, the nation's first ensuring cyber security & providing an alternate to GPS. #ISRO #ISIRI

Link: <https://www.isro.gov.in/News-Events/2022/ISIRI-India-20220922>

A Day Without Space GPS is Ground Zero for The New Space Race

Alternatives to GPS, collectively called Global Navigation Satellite Systems (GNSS), are growing rapidly because the old GPS system we rely on offers neither the precision nor security needed in an increasingly autonomous, risk-based, and globally connected world. #GPS #GNSS

Link: <https://www.fortune.com/story/2022/09/22/a-day-without-space-gps-is-ground-zero-for-the-new-space-race-1146282>



L3Harris breaks barriers in secure SATCOM with HAAM-R Modem at Northern Edge

L3Harris presented its Protected Tactical Waveform (PTW)-enabled HAAM-R modem. It provide warfighters long-range, higher-bandwidth communication in the presence of jamming across all domains. #L3Harris #AntiJamming

Link: <https://www.airforce-technology.com/news/l3harris-breaks-barriers-in-secure-satcom-with-haam-r-modem-at-northern-edge/>

